Constructing new APN functions from known ones

We present a method for constructing new quadratic APN functions from known ones. Applying this method to the Gold power functions we construct an APN function $x(3) + \text{tr}(x(9))$ over $\mathbb{F}_2(n)$. It is proven that for $n \geq 7$ this function is CCZ-inequivalent to the Gold functions, and in the case $n = 7$ it is CCZ-inequivalent to any power mapping (and, therefore, to any APN function belonging to one of the families of APN functions known so far).

General information
State: Published
Organisations: Discrete mathematics, Department of Mathematics
Contributors: Budaghyan, L., Carlet, C., Leander, G.
Pages: 150-159
Publication date: 2009
Peer-reviewed: Yes